1. Introduction

In this note I am interested in the $k = 2$ case of Vinogradov’s mean value theorem, the first nontrivial case. That is we seek to estimate the number of solutions to

\[ \begin{align*}
  x + y + z &= u + v + w, \\
  x^2 + y^2 + z^2 &= u^2 + v^2 + w^2, \\
  1 \leq x, y, z, u, v, w &\leq N, \\
  x, y, z, u, v, w &\in \mathbb{Z}.
\end{align*} \tag{1} \]

The number of such solutions is denoted $J_{3,2}(N)$. We remark that of all the nontrivial critical cases of Vinogradov’s mean value theorem, the case under current consideration is the only one where an asymptotic formula is known.

In what follows, we let $[N] = \{1, \ldots, N\}$.

2. The trivial solutions

We first indicate $6N^3 + O(N^2)$ trivial solutions to \( (1) \). Given any $x, y, z \in [N]$, we complete to a solution of \( (1) \) by choosing $u, v, w$ to be any permutation of $x, y, z$.

- If $x, y, z$ are distinct, there are 6 such permutations.
- If $|\{x, y, z\}| = 2$, there are 3 such permutations.
- If $x = y = z$, there is 1 such permutation.

The number of $x, y, z \in [N]$ such that $x, y, z$ are distinct is $N^3 + O(N^2)$, and so we conclude that

\[ J_{3,2}(N) \geq 6N^3 + O(N^2). \tag{2} \]

We show below that $J_{3,2}(N)$ is significantly larger than $6N^3$, that is there are many more solutions to \( (1) \) than these trivial solutions.
3. A PARAMETERIZATION OF SOLUTIONS

Our goal is to give a five parameter family of solutions to (1), which will be suitable for later analysis.

**Proposition 3.1** Suppose \(x, y, z, u, v, w \in \mathbb{Z}\) such that
\[
\begin{align*}
x + y + z &= u + v + w, \\
x^2 + y^2 + z^2 &= u^2 + v^2 + w^2,
\end{align*}
\] (3)

Then there are integers \(a, b, r, s, t\) such that
\[
(rb = sa) \text{ and } (x, y, z, u, v, w) = (0, a, b, b, 0, a) + (r, s, 0, r, s, 0) + (t, t, t, t, t, t). \tag{4}
\]

We remark that we have removed the condition that \(1 \leq x, y, z, u, v, w \leq N\) in Proposition 3.1. In this case any translate of a solution to (3) is also a solution, and thus we chose the letter \(t\) to indicate “translate.” We also remark that it is quick to verify that (4) is indeed a solution to (3).

**Proof.** Suppose \(x, y, z, u, v, w \in \mathbb{Z}\) satisfy (3). Let
\[
a = y - v, b = u - x, t = w + v - y, r = x - t, s = v - t.
\]

Then to establish (4), it is enough to check that \(rb = sa\), that is
\[
(x - t)(u - x) = (v - t)(y - v).
\]

But \(t = z + x - u = w + v - y\), and substituting according, we find we just need to check
\[
(u - z)(u - x) = (y - w)(y - v).
\]

This follows at once from the algebraic identity
\[
(a + b - c)^2 - (a^2 + b^2 - c^2) = 2(a - c)(b - c).
\]

\[\square\]

4. THE TRIVIAL SOLUTIONS REVISITED

It is not immediately evident what form the trivial solutions take in Proposition 3.1. They are
- \(b = a = 0\), giving rise to solutions \((r + t, s + t, t, r + t, s + t, t)\),
- \(b = s = 0\), giving rise to solutions \((r + t, a + t, t, r + t, a + t)\),
- \(r = s = 0\), giving rise to solutions \((t, a + t, b + t, t, a + t)\),
- \(r = a = 0\), giving rise to solutions \((t, s + t, b + t, b + t, s + t)\),
- \(r = a, b = s\), giving rise to solutions \((r + t, r + b + t, b + t, b + r + t, b + t, r + t)\),
- \(r = s, a = b\), giving rise to solutions \((r + t, a + r + t, a + t, a + r + t, r + t, a + t)\),
5. A LOWER BOUND FOR $J_{3,2}(N)$

With Proposition 3.1 in hand, we are sufficiently prepared to give a lower bound for $J_{3,2}(N)$.

**Theorem 5.1** One has

$$J_{3,2}(N) \geq \frac{3}{8\pi^2} N^3 \log N + O(N^3).$$

We remark that one has the more precise estimate

$$J_{3,2}(N) \sim \frac{18}{\pi^2} N^3 \log N,$$

but it will be clear from our arguments below that we are losing constants.

**Proof.** We assume at first that $4 \mid N$, for ease of argument, the general case following immediately. Our goal is to construct distinct solutions of the form (4), with suitable restrictions on the magnitudes of $a, b, r, s, t$.

We assume $1 \leq a, b, r, s \leq N/4$ and $1 \leq t \leq N/2$. Then all of the coordinates in (4) are at most $N$ in magnitude and thus contribute to $J_{3,2}(N)$. It follows that

$$J_{3,2}(N) \geq \frac{N}{2} \# \{(a, b, r, s) \in \mathbb{Z}^4 : rb = sa, 1 \leq r, b, s, a \leq N/4\}.$$

We set

$$M = N/4, \quad 1_M(x) := 1_{[1,M]}(x).$$

We then have (see Figure 1 for a picture)

$$\# \{(a, b, r, s) \in \mathbb{Z}^4 : rb = sa, 1 \leq r, b, s, a \leq N/4\} = \sum_{m \leq M^2} \left( \sum_{d \mid m} 1_M(d)1_M(m/d) \right)^2.$$

For integers $d_1, d_2$, we let

$$[d_1, d_2] := \text{lcm}(d_1, d_2).$$

We provide a string of equalities and explain the trickiest ones after.

$$\sum_{m \leq N^2} \left( \sum_{d \mid m} 1_M(d)1_M(m/d) \right)^2 = \sum_{d_1, d_2} 1_M(d_1)1_M(d_2) \sum_{m \leq M^2, d_1 \mid m, d_2 \mid m} 1_M(m/d_1)1_M(m/d_2)$$

$$= \sum_{d_1, d_2} 1_M(d_1)1_M(d_2) \left( \min \{M^2/[d_1, d_2], d_1 M/[d_1, d_2], d_2 M/[d_1, d_2]\} + O(1) \right)$$

$$= \sum_{d_1, d_2} 1_M(d_1)1_M(d_2) \left( \min \{d_1 M/[d_1, d_2], d_2 M/[d_1, d_2]\} + O(1) \right)$$

$$= 2 \sum_{1 \leq d_1, d_2 \leq M} d_1 M/[d_1, d_2] - \sum_{1 \leq d \leq M} M + O(M^2)$$

$$= 2M \sum_{1 \leq d_1 \leq d_2 \leq M} d_1/[d_1, d_2] + O(M^2).$$
The third inequality is a result of the fact $d_1, d_2 \leq M$, so the first term in the minimum is extraneous. The middle term the fourth line is the contribution from $d_1 = d_2$.

Thus

$$J_{3,2}(N) \geq \left( \frac{N^2}{4} \sum_{1 \leq d_1, d_2 \leq M} d_1/[d_1, d_2] \right) + O(N^3).$$

(5)

It just remains to estimate

$$\sum_{1 \leq d_1, d_2 \leq M} d_1/[d_1, d_2] = \sum_{1 \leq d_1, d_2 \leq M} (d_1, d_2)/d_2,$$

where

$$(d_1, d_2) := \gcd(d_1, d_2).$$
We have that
\[
\sum_{1 \leq d_1, d_2 \leq M} \frac{(d_1, d_2)}{d_2} = \sum_{1 \leq a \leq M} a \sum_{1 \leq d_1, d_2 \leq M, (d_1, d_2) = a} \frac{1}{d_2}
\]
\[
= \sum_{1 \leq a \leq M} \sum_{1 \leq t_2 \leq M/a} \frac{\phi(t_2)}{t_2}
\]
\[
= \sum_{1 \leq a \leq M} \sum_{1 \leq t_2 \leq M/a} \frac{\phi(t_2)}{t_2} \sum_{1 \leq a \leq M/t_2} 1
\]
\[
= \sum_{1 \leq t_2 \leq M} \frac{\phi(t_2)}{t_2} (\frac{M}{t_2} + O(1))
\]
\[
= M \left( \sum_{1 \leq t_2 \leq M} \frac{\phi(t_2)}{t_2} \right) + O(M)
\]
\[
= \frac{6}{\pi^2} M \log M + O(M).
\]
\[
= \frac{3}{2\pi^2} N \log N + O(N).
\]

We used that \( M = N/4 \) in the last step. The result follows from this estimate and (5).

We give some informal remarks. Note that we are seeking solutions to \( rb = sa \).
We have the obvious solutions \( r = s, b = a \). But we can also multiplicatively perturb \( r, b, s, a \) to obtain (many) nontrivial solutions.

6. A bound on a maximum

We set \( A = \{1, \ldots, N\} \). We set
\[
r_{3A,3A_2}(m, n) = \{ (x, y, z) \in A^3 : x + y + z = m, x^2 + y^2 + z^2 = n \}.
\]

Note we have
\[
J_{3,2}(N) = \sum_{m,n} r_{3A,3A_2}(m, n)^2 \leq 36N^3 \max_{m,n} r_{3A,3A_2}(m, n).
\]

Thus it is of interest to get upper bounds on the above maximum. For instance if one can show
\[
\max_{m,n} r_{3A,3A_2}(m, n) \ll N^\epsilon,
\]
then this gives rise to a good estimate for $J_{3,2}(N)$. It also provides more information than a mean value estimate.

**Proposition 6.1** With the notation above, we have

$$r_{3A,3A_2}(m, n) \ll \epsilon N^\epsilon.$$  

**Proof.** Fix $m$ and $n$ and assume

$$x, y, z \in [N], \quad x + y + z = m, \quad x^2 + y^2 + z^2 = n. \quad (6)$$

Let $X = 3x - m$, $Y = 3y - m$, $Z = 3z - m$. Then $X + Y + Z = 0$. On the other hand

$$X^2 + Y^2 + Z^2 = (3x - m)^2 + (3y - m)^2 + (3z - m)^2 = 9n - 3m^2,$$

and so

$$X^2 + XY + Y^2 = \frac{9n - 3m^2}{2}.$$  

This is the principal quadratic form of discriminant $-3$ (incidentally, (6) ensures that $n$ and $m$ have the same parity). Thus the number of integer solutions to $X, Y$ to the above equation is

$$\ll \epsilon n^\epsilon \ll N^\epsilon.$$  

Now $x = (X + m)/3$, $y = (Y + m)/3$, and $z = (Z + m)/3 = (-X - Y + m)/3$. Thus a choice of $X$ and $Y$ uniquely determines $x, y, z$ and so there are $\ll \epsilon N^\epsilon$ solutions to (6). □

7. GEOMETRIC RELATION TO THE PRINCIPAL QUADRATIC FORM OF DISCRIMINANT $-3$

We remark that the form $X^2 + XY + Y^2$ is somehow intrinsically related to (6). I actually started with (6) and used orthogonal transformations to bring the hyperplane to the $xy$-plane, and in the end, the whole problem reduced counting solutions to the same quadratic form. We explain very briefly, only giving the main points and leaving some (but not too many) of the details to the interested reader. An orthogonal matrix mapping the vector $[1, 1, 1]^T$ to $[0, 0, \sqrt{3}]^T$ is

$$P := \begin{bmatrix}
\sqrt{2}/\sqrt{3} & -\sqrt{2}/(2\sqrt{3}) & -\sqrt{2}/(2\sqrt{3}) \\
0 & \sqrt{2}/2 & -\sqrt{2}/2 \\
1/\sqrt{3} & 1/\sqrt{3} & 1/\sqrt{3}
\end{bmatrix} = \begin{bmatrix}
\sqrt{2}/\sqrt{3} & 0 & -1/\sqrt{3} \\
0 & 1 & 0 \\
1/\sqrt{3} & 0 & 2/\sqrt{3}
\end{bmatrix} \begin{bmatrix}
1 & 0 & 0 \\
0 & \sqrt{2}/2 & -\sqrt{2}/2 \\
0 & \sqrt{2}/2 & \sqrt{2}/2
\end{bmatrix}.$$  

Let $\vec{x} = [x, y, z]$. Then $\langle \vec{x}, \vec{x} \rangle = n$ if and only if $\langle P\vec{x}, P\vec{x} \rangle = n$. Also $\langle \vec{1}, \vec{x} \rangle = m$ if and only if $\langle [0, 0, 3/\sqrt{3}]^T, P\vec{x} \rangle = m$. Thus the last coordinate of $P\vec{x}$ is fixed, which is why we chose to map $[1, 1, 1]^T$ to $[0, 0, \sqrt{3}]$. Thus we have successfully mapped the three dimensional problem to a two dimensional problem. More precisely, we let

$$A := \begin{bmatrix}
3\sqrt{2}/(2\sqrt{3}) & 0 \\
\sqrt{2}/2 & \sqrt{2}
\end{bmatrix}.$$
We came to \( A \) by substituting \( z = -x - y \) in the expression \( P[x, y, z] \) and only considering the first two coordinates (the third coordinate is fixed). Then a straightforward calculation reveals that
\[
r_{3A,3A_2}(m, n) = \mathbb{Z}^2 \cap \{ \vec{y} : \langle A\vec{y}, A\vec{y} \rangle = n - (1/3)m^2 \}.
\]
But we see explicitly that \( \langle A\vec{y}, A\vec{y} \rangle = 2y_1^2 + 2y_1y_2 + 2y_2^2 \), and again we are lead to
\[
y_1^2 + y_1y_2 + y_2^2 = \text{constant},
\]
uncovering the principal quadratic form of discriminant \(-3\).

8. SYMMETRIES

What follows is just personal meanderings that I chose not to delete in the off-chance someone finds it of use. In all of the above arguments, symmetries of \( [1] \) played an important role in the arguments. In the first argument, translations were key, the second argument required affine transformations, while in the third argument we invoked orthogonal transformations.

Looking ahead to \( J_{k,k(k+1)/2}(N) \), for a general \( k \geq 3 \), it would be nice if one had such symmetries. Indeed we still have affine invariance (if one forgets about the archimedian conditions on the variables). The problem will surely be that this will not be enough symmetries to isolate the solutions, the way we did in Proposition 3.1.

**Question 8.1 (Broad)** Are there symmetries present in \( J_{3,6}(N) \) that will allow us to repeat some of the above arguments?

Note there are not many isometries of \( \ell_3(\mathbb{R}^d) \) (any isometry is linear by Mazur-Ulam). Nevertheless, we could, for instance, borrow an idea from additive combinatorics and consider something like a Freiman homomorphism, which there are plenty of (note a Freiman homomorphism need not extend to a linear isomorphism of the whole space).